Claims

1. A system for controlling access to files and application programs on a personal computing device, comprising:

A) a personal locking device comprising a 1st wireless data communication device, said 1st wireless data communication device having a 1st unique identifier associated therewith and having a capability to establish a wireless data link by a wireless communications protocol; and

B) a 2nd wireless data communication device integrated into or attached to said personal computing device, said 2nd wireless data communication device having a 2nd unique identifier associated therewith and having a capability to establish a wireless data link by said wireless communications protocol;

wherein said 1st and 2nd wireless data communication devices are configured to establish a wireless data link to each other based upon an exchange of said 1st and 2nd unique identifiers, and

said 2nd wireless data communication device is configured to monitor the quality of service of said wireless link and send a message to said personal computing device when said quality of service falls below a predetermined threshold.

2. The system of claim 1, wherein said personal computing device is selected from the group consisting of: notebook computers, desktop computers, tablet PC computers, server computers, personal digital assistants, and PocketPCs.

3. The system of claim 1, wherein said wireless data communication devices are radio frequency communication devices, said wireless data link is a radio

frequency data link, and said wireless communications protocol is a radio frequency communications protocol.

4. The system of claim 1, wherein said wireless data communication devices are Bluetooth data communication devices, said wireless data link is a Bluetooth data link, said wireless communications protocol is the Bluetooth communications protocol (IEEE 802.15), and said unique identifiers are Bluetooth device identification numbers that are uniquely assigned to each Bluetooth radio.

5. The system of claim 4, wherein said 2nd Bluetooth data communication device comprises a Bluetooth radio integrated into said personal computing device or a Bluetooth dongle that is attached to a port of said personal computing device.

6. The system of claim 1, wherein said personal locking device is selected from the group consisting of: cell phones, Smartphones, Pocket PC portable computers, and personal digital assistants (PDAs).

7. The system of claim 4, wherein said 1st Bluetooth data communication device comprises a Bluetooth radio module.

8. The system of claim 7, wherein said 1st Bluetooth data communication device additionally comprises a microcontroller and a software installed on said microcontroller for controlling said Bluetooth radio module.

9. The system of claim 7, wherein said 1st Bluetooth data communication device additionally comprises a software program for controlling said Bluetooth radio module.

10. The system of claim 1, wherein said personal locking device additionally comprises a user input means for sending a message to said 2nd wireless communications device.

11. The system of claim 10, wherein said user input means is selected from the group consisting of: a button, a switch, a dial, a touchpad, a keyboard, and a fingerprint sensor.

12. The system of claim 10, wherein said message is a message that requests said personal computing device to go into a locked state in which access to its files and application programs is prohibited or restricted.

13. The system of claim 10, wherein said message is a message that requests said personal computing device to go into an unlocked state.

14. The system of claim 10, wherein said message is a message that requests said personal computing device to go into an unlocked state upon receipt of a user input at said personal computing device.

15. The system of claim 14, wherein said user input comprises a correct personal access code (PAC) or inputs at the keyboard or mouse associated with said personal computing device.

16. The system of claim 1, additionally comprising an access control software program installed on said personal computing device, said software program comprising:

A) a means to configure said 1st and 2nd wireless communication devices to establish said wireless link between them;

B) a means to receive messages from said 2nd wireless communication device; and

C) a means to place, in response to a message from said 2nd wireless communication device, said personal computing device in a locked state in which access to its files and application programs is prohibited or restricted.

17. The system of claim 16, wherein said software program additionally comprises a means to configure said 2nd wireless communication device to monitor said quality of service of said wireless link.

18. The system of claim 16, wherein said software program additionally comprises a means to place, in response to a message from said 2nd wireless communication device, said personal computing device in an unlocked state.

19. The system of claim 16, wherein said software program additionally comprising a means to place, in response to a message from said 2nd wireless communication device and a user input to said personal computing device, said personal computing device in an unlocked state.

20. The system of claim 19, wherein said user input comprises a correct personal access code (PAC) or inputs at the keyboard or mouse associated with said personal computing device.

21. A method for controlling access to files and application programs on a personal computing device, comprising the steps of:

A) providing a personal locking device comprising a 1st wireless data communication device, said 1st wireless data communication device having a 1st

unique identifier associated therewith and having a capability to establish a wireless data link by a wireless communications protocol;

B) positioning said personal locking device in the operating space of said personal computing device;

C) providing a 2nd wireless data communication device integrated into or attached to said personal computing device, said 2nd wireless data communication device having a 2nd unique identifier associated therewith and having a capability to establish a wireless data link by said wireless communications protocol;

D) configuring said 1st and 2nd wireless data communication devices to establish a wireless data link to each other based upon an exchange of said 1st and 2nd unique identifiers, thereby authorizing said personal locking device for said personal computing device;

E) configuring said 2nd wireless data communication device to monitor the quality of service of said wireless link and send a message to said personal computing device when said quality of service falls below a predetermined threshold;

F) establishing said wireless data link;

G) monitoring said quality of service of said wireless data link; and

H) sending said message when said quality of service falls below said predetermined threshold.

22. The method of claim 21, additionally comprising the steps of:

A) requesting a user to establish a personal access code (PAC);

B) receiving said code and associating said code with said wireless link; and

C) storing said code in said personal computing device.

23. The method of claim 21, additionally comprising the steps of:

A) positioning a personal locking device in the operating space of said personal computing device;

B) determining whether said personal locking device is an authorized personal locking device for said computing device;

C) establishing a wireless data link between said 2nd wireless data communication device and the wireless data communication device of said personal locking device;

D) monitoring the quality of service of said wireless data link;

E) receiving a message from said 2nd wireless communication device when said quality of service rises above a predetermined threshold; and

F) placing said personal computing device in an unlocked state in response to said message.

24. The method of claim 21, additionally comprising the steps of:

A) positioning a personal locking device in the operating space of said personal computing device;

B) determining whether said personal locking device is an authorized personal locking device for said computing device;

C) establishing a wireless data link between said 2nd wireless data communication device and the wireless data communication device of said personal locking device;

D) monitoring the quality of service of said wireless data link;

E) receiving a message from said 2nd wireless communication device when said quality of service rises above a predetermined threshold;

F) detecting a user input at said personal computing device; and

G) placing said personal computing device in an unlocked state in response to said message and said detection of user input.

25. The method of claim 24, wherein said step of detecting user input comprises detecting keystrokes at the keyboard or movement or clicking at the mouse associated with said personal computing device.

26. The method of claim 21, additionally comprising the steps of:

A) positioning a personal locking device in the operating space of said personal computing device;

B) determining whether said personal locking device is an authorized personal locking device for said computing device;

C) establishing a wireless data link between said 2nd wireless data communication device and the wireless data communication device of said personal locking device;

D) monitoring the quality of service of said wireless data link;

E) receiving a message from said 2nd wireless communication device when said quality of service rises above a predetermined threshold;

F) requesting a user to input a personal access code;

G) receiving said user input;

H) comparing said user input to the personal access code that is stored in said personal computing device; and

I) placing said personal computing device in an unlocked state if there is a match between said input and said stored personal access code.

27. The method of claim 21, wherein said personal computing device is selected from the group consisting of: notebook computers, desktop computers, tablet PC computers, server computers, personal digital assistants, and PocketPCs.

28. The method of claim 21, wherein said wireless data communication devices are radio frequency communication devices, said wireless data link is a radio frequency data link, and said wireless communications protocol is a radio frequency communications protocol.

29. The method of claim 21, wherein said wireless data communication devices are Bluetooth data communication devices, said wireless data link is a Bluetooth data link, said wireless communications protocol is the Bluetooth communications protocol (IEEE 802.15), and said unique identifiers are Bluetooth device identification numbers that are uniquely assigned to each Bluetooth radio.

30. The method of claim 29, wherein said 2nd Bluetooth data communication device comprises a Bluetooth radio integrated into said personal computing device or a Bluetooth dongle that is attached to a port of said personal computing device.

31. The method of claim 21, wherein said personal locking device is selected from the group consisting of: cell phones, Smartphones, Pocket PC portable computers, and personal digital assistants (PDAs).

32. The method of claim 29, wherein said 1st Bluetooth data communication device comprises a Bluetooth radio module.

33. The method of claim 32, wherein said 1st Bluetooth data communication device additionally comprises a microcontroller for controlling said Bluetooth radio module.

34. The method of claim 32, wherein said 1st Bluetooth data communication device additionally comprises a software program for controlling said Bluetooth radio module.

35. The method of claim 21, wherein said personal locking device additionally comprises a user input means for sending messages to said 2nd wireless communications device.

36. The method of claim 35, wherein said user input means is selected from the group consisting of: a button, a switch, a dial, a touchpad, a keyboard, and a fingerprint sensor.

37. The method of claim 35, additionally comprising the steps of:

A) sending a message requesting said personal computing device to go into a locked state in which access to its files and application programs is prohibited or restricted; and

B) placing said personal computing device in a locked state.

38. The method of claim 35, additionally comprising the steps of:

sending a message requesting said personal computing device to go into an unlocked state; and

placing said personal computing device in an unlocked state.

39. The method of claim 35, additionally comprising the steps of:

sending a message requesting said personal computing device to go into an unlocked state;

receiving a user input at said personal computing device; and placing said personal computing device in an unlocked state upon receipt of said message and said user input.

40. The method of claim 39, wherein said step of receiving user input comprises detecting keystrokes at the keyboard or movement or clicking of the mouse associated with said personal computing device.

41. The method of claim 35, additionally comprising the steps of:

A) sending a message requesting said personal computing device to go into an unlocked state;

B) requesting a user to input a personal access code;

C) receiving said users input;

D) comparing said input to the personal access code that is stored in said personal computing device; and

E) placing said personal computing device in an unlocked state if there is a match between said input and said stored personal access code.

42. The method of claim 21, additionally comprising the steps of:

A) installing an access control software program on said personal computing device;

B) using said program to configure said 1st and 2nd wireless communication devices to establish said wireless link between them;

C) using said program to receive messages from said 2nd wireless communication device; and

D) using said program to place, in response to a message from said 2nd wireless communication device, said personal computing device in a locked state in which access to its files and application programs is prohibited or restricted.

43. The method of claim 42, additionally comprising the step of:

A) using said program to configure said 2nd wireless communication device to monitor said quality of service of said wireless link.

44. The method of claim 42, additionally comprising the steps of:

A) using said program to receive a message from said 2nd wireless communication device; and

B) placing said personal computing device in an unlocked state upon receipt of said message.

45. The method of claim 42, additionally comprising the steps of:

A) using said program to receive a message from said 2nd wireless communication device;

B) using said program to receive user inputs to said personal computing device;

C) using said program to place, in response to said message and said user input, said personal computing device in an unlocked state.

46. The method of claim 45, wherein said step of receiving user inputs comprises the step of detecting keystrokes at the keyboard or movement or clicking of the mouse associated with said personal computing device.

47. The method of claim 42, additionally comprising the steps of:

A) using said program to receive a message from said 2nd wireless communication device;

B) requesting a user to input a personal access code;

C) receiving said user input;

D) comparing said user input to the personal access code that is stored in said personal computing device; and

E) placing said personal computing device in an unlocked state if there is a match between said input and said stored personal access code.